INTERNAL INSPECTIONS REPORT

HEADQUARTERS OFFICE

Prepared By:
[Insert Agency]
[Insert Agency Address]

[Insert Date]

INSTRUCTIONS

The following questions serve as an internal audit checklist regarding the agencies security procedures relating to Internal Revenue Service documents and federal security implementation controls. The purpose of this questionnaire is to measure the agencies level of compliance with federal disclosure regulations.

When answering the questions in this document, the answers should be entered on the line directly below the question. Formatting and color for the answer has already been set, so modifying this it not advisable. The responses will be colored blue, so it's easily identifiable. For Example:

1. How is FTI received from the IRS?
   FTI is received from the IRS via the secure Tumbleweed client to a Windows XP workstation.

After completion, the form should be printed out and signed by the Disclosure Officer and the Director from the Agency.

The Agency should complete the contact information below for all parties that involved in supplying information.

Name	Title	E-mail

It is advisable for the agency to collect and maintain documented evidence to back to answers to this report in the instance of an audit. Having this evidence on hand will also aid the IRS Safeguards on-site review.

Record Keeping Requirements (Publication 1075 section 3.0) IRC Section 6103(p)(4)(A)

1. How is FTI received from the IRS? (Tumbleweed, ConnectDirect, other Secure Data Transmission (SDT)-list)

2. Are FTI receipts logged ?

    a. What data elements are captured in the log?

3. Are products/documents created from the FTI data (letters, reports, etc.)? Describe what products/documents are created.

    a. How are these products/documents tracked and stored until destruction?

4. Upon receipt of FTI, how and where is the data electronically distributed?

5. What type of FTI is received from the IRS?

6. Are back-up files stored off-site?

    a. Where (Site Name and address) are files stored?

    b. What protections are in place?

    c. Who currently has access (name & title)?

Secure Storage (Publication 1075 section 4.0) IRC Section 6103(p)(4)(B)

7. Please describe the physical security of the Agency Headquarter? (e.g. keypad locked doors, guard desks, locations, hours, etc.)

    a. If keypads are used, is each attempt logged?

    b. Who reviews the access attempt logs? (Name and title)

8. What alarm systems are currently running at Agency Headquarters? (e.g. Intrusion Alarms, Motion Detectors, Exit Alarms)

    a. Who monitors these alarms? (Name and title)

9. Are security cameras used at the Agency Headquarters?

    a. Who monitors the security feed? (Name and title)

10. Are records maintained on the issuance of keys/key cards?

    a. How are records maintained? (automated file, written log, etc.)

    b. Who is responsible for the issuance of keys/key cards (Name and title)

    c. Are periodic reviews conducted to reconcile records and determine if users still need access?

        i. Date of last review.

11. Is FTI locked in a storage cabinet?

    a. Where is the key kept?

b. Who has access to the key?

c. How many keys are in existence?

d. Who maintains the backup keys?

12. Are combination locks used?

a. How often is the combination changed?

b. Who controls the combinations?

13. Are ID cards required to be worn by employees at all times?

a. How are ID cards inventoried or managed?

14. Do visitors/vendors sign a visitor access log?

a. What data elements are captured in the log?

b. Who reviews the visitor access log periodically?

15. Two barriers are required to protect FTI. Please Describe the one that applies to your agency:
i. Secured perimeter / locked container
ii. Locked perimeter / secured interior
iii. Locked perimeter / secured container
iv. Other (describe)

16. Who has access to the office after core business hours?

    a. How is security enforced after core business hours?

17. Are files stored at an off-site storage facility?

18. Is this a state-run facility or a contractor site?

    a. How access limited from non-agency personnel?

19. How are the files shipped / transferred to the off-site storage facility?

Restricting Access (Publication 1075 section 5.0) IRC Section 6103(p)(4(C)

20. What identifying information is used to retrieve FTI?

21. Is FTI kept separate or is it commingled with other information?

22. Can FTI within agency records be located and separated easily?

23. After independent verification occurs, what specific data is entered into the system?

24. How is access limited to authorized personnel?

25. Is FTI made available to personnel outside of agency personnel (contractors, other agencies, etc.)?

a. List personnel/offices and provide a justification.

26. Does the agency have web based applications?

a. Is FTI accessible through a web site?

27. Are FTI access log reports monitored to detect unauthorized browsing?

28. Is FTI transmitted via email?

a. How is the FTI protected? (encryption - describe)

29. Is FTI transmitted via fax machine?

a. Where is the receiving fax machine located? (location in office)

b. Are all individuals in the receiving location cleared for FTI access?

Disposing Federal Taxpayer Information (Publication 1075 section 8.0) IRC Section 6103(p)(4)(F)

30. Is FTI paper waste material generated?

a. Where is paper waste material placed? (recycle bins, locked containers, waste baskets, other container)

b. How is the paper waste material destroyed?

c. Who performs the destruction of paper waste material? (Agency Staff, Contractor – list)

d. Is a contractor used to pick up the waste material?

i. Name of contractor:

ii. Where does the contractor take the waste material for destruction?

iii. Does agency staff accompany material and view destruction?

Computer System Security (Publication 1075 section 5.6)

31. Are there user accounts for the application containing FTI?

a. How are these accounts managed?

b. Who manages the accounts?

c. Are accounts given the appropriate level of permissions that do not exceed a persons need for their job functions?

d. How often and by whom are accounts reviewed for access need?

e. Are accounts configured to lock after 3 failed login attempts?

32. Are application users supplied with unique user IDs?

a. How does the user receive their network user ID?

b. Are user IDs disabled after 90 days of inactivity?

c. Are user IDs archived?

33. Are application passwords set to be a minimum of 8 characters in length?

a. What complexity requirements are tied to passwords?

b. Are passwords required to be changed at least every 90 days?

c. How many generations of passwords are maintained?

34. Is an IRS approved warning banner displayed prior to a user application?

35. Is the application configured to lock/terminate the session after 15 minutes of inactivity?

36. Is auditing enabled on the application?

a. What auditable events are set to be captured?

b. Is appropriate storage capacity given to audit records?

c. Are there alerts established to inform administrators of an audit processing failure?

i. How is the administrator alerted?

d. Does the application provide capabilities for monitoring, analyzing, and report generation of auditable events?

i. Does the reporting feature allow for reduction, so that reports on specific audit events can be tailored to a report?

e. Are time stamps used with each audit event?

f. How is the audit information protected?

g. How long are audit records maintained?

37. Does the Agency provide annual security awareness training?

a. Are there records maintained to track employee completion of this training?

38. Does the Agency provide job-related security training?

a. Are there records maintained to track employee completion of this training?

39. Does the Agency utilized the Plan of Actions and Milestones (POA&M) process to manage risks identified through security assessments or risk assessments?

40. Is a baseline configuration maintained for the application that contains software versions, patch levels, services used, etc.?

41. Does the Agency follow a configuration change control process?

a. How are change requests submitted?

b. Who analyzes the requests?

c. Is there an established Configuration Control Board that is involved in the approval process?

d. Are all changes to the information system documented?

42. Is there a list of personnel who are authorized to make changes to the application?

a. Is this list of personnel periodically reviewed?

43. Does the Agency have an implemented Incident Response process?

a. Does the Agency track and document security incidents on an ongoing basis?

b. Does the Agency promptly report incidents involving FTI to TIGTA?

44. Are Risk Assessments conducted with results documented?

a. How often are Risk Assessments conducted?

b. What is the date of the last Risk Assessment?

45. Is the application managed using a System Development Life Cycle (SDLC) methodology that is consistent with NIST SP 800-64?

I hereby submit this Internal Inspections Report to the headquarters function of this agency as part of the IRS Safeguards Internal Inspections requirement

/s/

_____ _____

HQ Office Official Conducting Internal Inspection Date

I acknowledge that I reviewed this Internal Inspections Report as part of the IRS Safeguards Internal Inspections requirement and initiated appropriate corrective actions for any deficiencies identified.

/s/

_____ _____

Agency Disclosure Officer Date

/s/

_____ _____

Agency Official Date